CLAIMS

What is claimed is:

1. An online transaction method for providing a user with an online transaction via a digital media in an online transaction system, the online transaction system comprising a certificate authority module, at lease one service provider module, at lease one management module and a transaction module, each management module respectively having an authentication device and a transaction device, the authentication device being connected between the service provider module and the certificate authority module, the transaction device being connected between the service provider module and the transaction module, the online transaction method comprising:

registering a digital certificate in the certificate authority module by the user via the digital media for generating a log data, the certificate authority module outputting the log data to the authentication device of the management module in a predetermined period;

inputting the digital certificate in the service provider module by the user via the digital media for generating a digital signature, the service provider module outputting the digital signature to the authentication device of the management module;

authenticating the digital signature according to a predetermined procedure for generating an authentication code;

verifying the effectiveness of the user's authentication in the service provider module, and providing the user with the online transaction for generating a corresponding first transaction data to the transaction module;

processing the first transaction data in the transaction module for generating a second transaction data to the transaction device of the management module;

recording the second transaction data in the transaction device, and outputting the second transaction data to the service provider module; and

displaying the second transaction data in the service provider module;

wherein the digital signature, the authentication code, the first transaction data and the second transaction data are respectively based on the digital certificate for encryption in the transmission process of the online transaction system.

2. The online transaction method of claim 1 wherein the authentication device and

the transaction device independently operate in the management module.

3. The online transaction method of claim 2 wherein each management module respectively manages a plurality of corresponding digital media, the user registers a corresponding digital certificate in the certificate authority module via the corresponding digital media for generating a corresponding log data stored in the certificate authority module and the authentication device of the corresponding management module respectively.

4. The online transaction method of claim 3 wherein the predetermined procedure comprises the steps of:

(a) checking whether the corresponding relationship between the digital certificate and the management module exits; and

(b) if YES in step (a), authenticating the digital signature with the corresponding log data stored in the corresponding authentication device for generating the authentication code, and outputting the authentication code to the service provider module.

5. The online transaction method of claim 4 wherein if No in step (a), outputting the digital signature to the certificate authority module, authenticating the digital signature with the corresponding log data stored in the certificate authority module for generating the authentication code, and outputting the authentication code to the service provider module.

6. The online transaction method of claim 2 wherein the predetermined procedure comprises the step of authenticating the digital signature with the log data stored in the authentication device for generating the authentication code, and outputting the authentication code to the service provider module.

7. The online transaction method of claim 1 wherein the online transaction system further comprises a virtual account module connected to the transaction module for providing an account data, the user updating the account data according to a predetermined method.

8. The online transaction method of claim 7 wherein the predetermined method comprises the step of updating the account data by an automated teller machine.

9. The online transaction method of claim 1 wherein the digital media can be a smart card.

10. The online transaction method of claim 1 wherein the digital media can be a biological identification device.